

IT POLICY MANUAL

This manual has been designed for information retention and comprehension; assuming, of course, that each employee has at least the most basic of concepts committed to memory.

Therefore, if you cannot answer the following simple question, you will not be allowed to read any further...

and you will be put in Time-Out for 10 minutes.

Good Luck! Everyone is watching you.

WEEDING OUT SURVEY

What does IT stand for, anyway?

Circle the correct answer.

- A. Irritating Techno-Geeks**
- B. Invisible Toads**
- C. Information Technology**
- D. All of the Above**

The correct answer is C.

However, credit will be given if you chose D.

1



"This one comes with free 'What-Would-Jesus-Download?' software."

General

We have invested considerable time, money, and people resources into providing computer hardware, software, and networking to equip the staff and volunteers to perform their varied functions. However, employment here does not guarantee access to a computer or related resources. As an employee or volunteer, it is your responsibility to take reasonable efforts to safeguard the valuable equipment and data provided to you.

Staff members and volunteers are representatives of the Church. Any use of computer equipment is an extension of that representation. With access to email and the internet, you can represent the Church, worldwide, nearly instantly. All access needs to be minimally "appropriate," and preferably of a positive nature.

Our policies are intended to protect both the Church and the computer user. Violation of policies is grounds for disciplinary action, which may include termination. Violation of some policies may also call for additional legal or civil actions. Exceptions are handled only by PRIOR request and approval of the IT Department. Requests should be made by way of email addressed to the helpdesk.

Policies are detailed below. Your failure to read or understand these policies does NOT negate them!

WEEDING 2:

Hardware, to a geek, means:

- A. Rough handling of computer
- B. Dressing up
- C. Computer components
- D. Pocket Protectors

ANSWER: C

Hardware

Your computer is the property of the Church. Adding hardware to, reconfiguring hardware on, or removing hardware from your computer is prohibited. If you feel that the hardware needs attention, please request assistance from the IT Department. This means (for desktop users) that you should not move your hardware from one area of the building to another without authorization from IT. Neither should you "swap" hardware from your computer to/from any other computer within the organization without prior consent.

Computer settings and configurations are not to be modified or adjusted by any user.

Software

All authorized and approved software has been pre-loaded onto your computer before you received it. With very few exceptions (and you must have approval), you are not to load any additional software onto your computer. This includes screensavers, shareware programs, your own personal copy of anything (again, unless approved), utilities, drivers, etc. If you need/want to load something, please obtain permission from the IT Department. Be prepared to provide a valid reason that has to do with your productivity or the needs of your Department within the organization. Games are prohibited, as they tend to pull our attention and time away from our work.



Unauthorized Software

Unauthorized software may be removed without warning. If a user installs software that causes a problem with the normal use of the computer, the IT Department will not treat this as an emergency. Restoration of normal operation will take place when time is available and it is very possible that the not all previous functionality will EVER be restored. Any items stored on the local disk drive, including data, may be lost forever.

Problems with Nonstandard Software

Nonstandard software requires a disproportionate amount of time to install and support. Requests for the user's personal convenience will not be approved. This includes software such as Quicken or tax preparation programs. If disk space becomes an issue on your computer, you may be asked to remove non-standard programming from your hard drive. Desktop users are not permitted, under any circumstances, to load programs onto computers without prior permission from the IT Department.

Data

Your computer and all the software contained on it or on the network servers are the property of the Church. This is true whether created by you or someone else. Except in circumstances where specific Intellectual property rights exists, the data files on the network also belong to the Church. You should use caution when creating files that reside either on your computer or on the network that are of a highly personal nature. We do not guarantee privacy or continued access to any material created or placed on the network or placed on your hard drive.

In general, security has been established to protect those files from unauthorized access, modification, or accidental deletion. However, we reserve the right to inspect and/or open any data files which reside on the network, including local hard drives at any time. It is not our intent to "spy" (and we do not routinely inspect files), but only to reserve the right to maintain the policies set forth in this document.

'Data' is plural.
Do you know what the singular tense is? Did you pay attention in Latin class way back when?

ANSWER: We're not talking about many hoo.

3

FAQ

"How come everyone has the same password of six asterisks?"

ANSWER:

Go into Time-Out.

Physical Security

Employees are expected to take reasonable measures to protect computers, data, and the network, from unauthorized access. For desktop users, this means properly guarding passwords, locking doors as appropriate, and being aware of non-Staff member using Church resources (computers). Notebook users need to be much more proactive about security. (Approximately 1 in 14 notebook computers are stolen nationwide. Church owned notebooks have been stolen in the past!) Notebooks must NEVER be left in an unattended area. This includes leaving systems on a desk overnight, even if the office is locked. Leaving a system on a desk, even during the day, when it is not certain that other Staff members are near by is equally risky. Unattended, at risk systems, are subject to confiscation. Likewise, they should never be checked as baggage nor left visible in an unattended car. Desktop computers are for employee use only - NOT for family and friends.



PART 2

Network Security

The IT Department (Information Technology) has taken every precaution to protect our network and its data from purposeful or accidental damage or destruction. The key element in that security model is your login name and password. Each login name/password combination gives different and specific rights and permissions to access network resources to each user (e.g. you have different access rights than another Staff member might). Therefore, sharing your login name or password with anyone (including staff members) is strictly prohibited. Allowing someone to use your computer logged on as you (e.g. you let them sit down at your computer without you logging off) is also prohibited.

If an authorized user needs to use your computer, you must log off and let them log on as themselves. If an unauthorized user (one who does not have their own login name and password) wishes to use your computer or the network, you must send an email request to helpdesk asking that an account be created for that person. This request should be made in advance. There are no exceptions to this requirement (spouses, children, or any other family relationships do not extend to them rights to use the network!) This includes notebooks that are many times used within the home. The equipment and its contents continue to be a part of our network regardless of where they are used.

The Internet

Access to the Internet has been given to you primarily to assist in your job. If it can be a convenience to you in your personal life, that is all right, with some caveats. Our responsibility to the organization, each other, and to the God that we serve is to make the best use of our time while we are here. With that in mind, the following are the positions of the leadership:

Restrictions and Cautions:

- Excessive surfing the web for personal reasons is to be avoided at all times. Excessive is a judgement call; use good judgement. If you are surfing for non-ministry related reasons for more than 15 minutes per day, you should be aware that you are beginning to infringe on your employer's time.
- Viewing or downloading of materials or Internet sites that would not be glorifying to God or edifying to others is strictly prohibited. A definition of unacceptable site content can be provided upon request, but most of you will know this instinctively.
- Downloading and then installing programs from the Internet onto your computer is strictly prohibited. This includes games, "trial" versions of software, fonts, sounds, graphics, shareware programs, etc.
- Use of "streaming media" (including networked radio broadcasts, video clips, audio clips, and similar media content) is not allowed during normal business hours because of the bandwidth requirements... which means it slows everything down for the rest of us.
- Chat areas of the Internet are not a good use of our time and are therefore, prohibited unless a valid reason can be given to use them (there won't be many).
- Programs that constantly access the Internet for information updates (e.g. PointCast) must be set to update only twice during the business day or not be used at all. This leaves our network available for applications such as Shelby. Violators will be asked and required to remove the program if cooperation is not received in this area.
- We reserve the right to audit Internet use, including websites visited, as an accountability tool for those Staff that might be tempted to get into areas they shouldn't.



some of the TEN IT COMMANDMENTS

1. ***Thou shalt not*** divulge thy log-in or password.
2. ***Thou shalt not*** write thy password on a post-it note and stick it to thy monitor.
3. ***Honor*** the IT policies
4. ***Thou shalt not*** download anything... **ever.**
5. ***Thou shalt not*** surf the web to excess.
6. ***Honor*** thy equipment.
7. ***Thou shalt not*** install software illegally on thy computer.

to be continued...

In general, use caution and good judgement when using the Internet. It can be a wonderful tool for all of us, but can also wreak havoc with our network, productivity, and principles if left unchecked.

5



the rest of the
**TEN IT
COMMANDMENTS**

8. *Thou shalt not*
listen to thy CDs
loudly in thy cubicle.

9. *Thou shalt not*
ever subject thy
neighbors to your CD
of the "Cats"
soundtrack.

10. *Do not take* the
Microsoft name in
vain.

Working Environment

We want to provide a fun, yet productive environment in which our computer users can work. For that reason, it is requested and expected that you will use the multi-media capabilities of your computer wisely. Many of you will have sound capabilities in the form of CD-ROM drives, speakers, sound cards, and other equipment as appropriate. This is a privilege, not a right. Some of you will want to put sounds that are heard when certain actions are taken on your computer or you may want to play music via your computer using the CD-ROM drive. Other examples might be screensavers that make login or logoff sounds, etc.

All of these things are good and we want you to be able to take advantage of them to enliven your work experience. However, we ask and require that you keep the noise levels to a minimum for the benefit of you, those who work around you, and the visitors that are often in and around our offices. A good "Rule of Thumb" is that if a sound can be heard clearly when standing three feet outside of your office or cube, it's probably too loud for the work environment. Also, annoying or offensive sounds should never be utilized. And last, if you are asked to turn down your system, please respond with courtesy and understanding. Many people cannot fully concentrate on tasks when hearing continuous music or computer sounds.

WEEDING 3:

**When is it
appropriate to
forward an
internet joke to
your co-workers?**

A. When it's really
funny.

B. Never.

C. Only when you
use "Church Staff"
and then DELETE
anyone in IT off the
list.

D. Refer to "B".

ANSWER: B or D

Appropriate Use

Computers, like most other things, are tools that can be abused. When attached to the Internet, as our computers are, abuse can be very counter-productive, embarrassing to the Church, or even illegal. Internet access is primarily for work, but there are valid reasons for personal use. Specifically, we all have reasons to reach out to other people -- personal contact is part of the job. Some appropriate usage guidelines:

- Limit use of non-business email lists, especially joke lists. A joke that you wish to share can be forwarded to the Humor folder in Outlook Public Folders.
- Prayer request for persons not in your immediate family can be sent to the distribution list named Prayer Warriors. Doing so also sends the request to the Outlook Public Folder named Prayer Requests.
- In general, limit (to zero) forwarding of non-business email.
- Whenever possible, distribute links, not documents.
- Internal email list names (such as Church Staff) need to be protected.

Virus Protection

We have installed virus protection on many levels. All email messages, downloads, and files are scanned when received. If one of these contains a virus, the program first attempts to remove the virus from the item. If successful, the item is delivered into the recipient's mailbox and browser. If it cannot be extracted, the item is placed where it cannot be accessed and the IT Department is notified. We also have virus files on your local computer. The system regularly (daily) attempts to scan your local computer for virus files. All diskettes, CDs, or other media that your computer accesses are scanned before being opened This is another way we attempt to protect our network.

Attachments to Email Messages

Attachments to an email message could contain a virus that would:

- harm your computer
- harm everyone else on the network
- send itself automatically to everyone in your address book (hundreds of names including the Elders and Deacons).

To prevent this from happening, inspect each attachment using the three step rule, even if you think you can see the final ending of the file name.

1. Right-click on the attachment
2. Choose Save As...
3. Examine the final ending of the File name and compare to the list below. If the Save Attachment dialog box shows the attachment is on the Only Open list, press the Esc key and open the attachment. ONLY OPEN an attachment if the file name ends in one of the following:

.bmp	.lnk	.pps	.url	.eml	.mp3	.ppt	.wav
.doc	.mpg	.pub	.wpd	.gif	.msg	.rtf	.wps
.htm	.pcx	.tif	.xls	.jpg	.pdf	.txt	.xnk

Important Guidelines

- Our most important line of defense against a computer virus is users who follow these rules.
- These instructions must be followed even if the email is from a trusted source.
- These instructions must be followed even if you think you can see the full name of the attachment.
- Be suspicious even if you know and trust the sender.
- If you receive a warning that an attached file contains a macro, DISABLE the macro.



10. Computers have minds of their own.
 9. Antibiotics cure viruses.
 8. "Operator Error" refers to the phone.
 7. Clicking the mouse 20 times makes it go faster. (See the Law of Elevator Buttons).
 6. A softdrive is the opposite of a harddrive.
 5. Computers are possessed.
 4. USB is a TV channel.
 3. Solitaire is not addicting.
 2. Pounding on your keyboard is therapeutic.
- And the Number One Computer Misconception:**
1. Everyone needs a Palm Pilot.

7

Did you know?

Did you know that computers are mentioned in the Bible? Really!

3 BOOLEAN F10

A Letter from Paul to the Geeks:

"Remember, then, who entrusted you with such technology..."

Repairs and Maintenance of Computers

If you experience problems with your computer or any computer-related device (printers, monitors, etc.) contact the IT Department immediately. Repairs can be as simple as a loose cable or as complex as having to rebuild an entire system. Not all repairs and upgrades can be handled the same day or hour that they are reported. The IT Department will assess the situation and determine the course of action.

If you feel that you need different equipment than you currently have, contact the IT Department to discuss your needs and your request will be assessed and if approved, acted on in a timely manner if approved.

The IT Department, designated individuals, or approved vendors are the ONLY ones that are allowed to service any computer equipment that the Church owns. You are in no way allowed to open computer cases, remove computer cards, install computer cards, remove or replace cables, or other equipment from within or attached to any computer. If you have a problem, call the IT Department and let them take care of it.

End of Employment

Upon conclusion of employment here, your login rights and email address will be deactivated and your personal directory will be removed from the network. Files cannot be removed from the network without the express approval of the IT Department and the leadership of the Church.

Resources and IT Training

Each computer user is required to demonstrate their mastery of certain computer skills. The Network Introductions Class and the Outlook Introduction Class are offered to help users learn or review these skills. Most users attend these two classes, but an "Advanced Placement" option is also available. After this material is mastered, optional classes are available.

The answers to many IT questions are contained in an Outlook Public Folder named the Staff Knowledge Base.



Is God a dot com
or a dot org?

So now what?

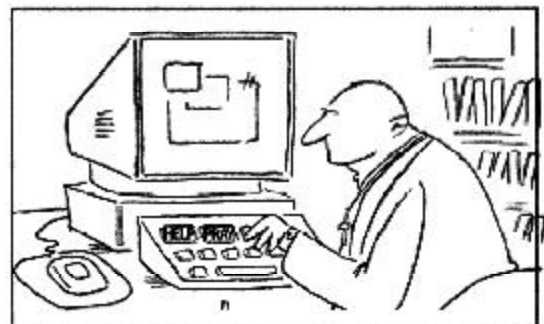
What IT is doing

In December, 2001, we introduced a tool to help eliminate a lot of the spam (aka junk mail, or UCE - Unsolicited Commercial Email) that has been coming into our email mailboxes. This isn't a 100% solution, but it should help. This anti-spam tool uses technology in two ways: first, it compares messages to a list of well-known spam sources and deletes any such messages before they ever come to you. Secondly, it does some examination of words and phrases within a message, and when "inappropriate" text is found, the message is quarantined and a replacement message is delivered, indicating the message was stripped. This word/phrase filtering covers the following broad categories: Profanity, Racial Discrimination, Sexual Discrimination, Hoaxes, Chain Mail, Melissa Virus, and HTML Scripting.

What you can do to help

There are also a lot of things you can do to help control spam. Consider that one of the things a spammer is most looking for is a list of valid email addresses. Here are a few suggestions:

- If you are sending a message to dozens (or hundreds!) of email addresses, hide those addresses! If that message gets to a spammer, he's just harvested all those addresses and will be sending his junk to all of your friends and contacts.
- Likewise, if you are forwarding on a message that already has lots of email addresses in it (this is a questionable thing to do in the first place, but that's another story), PLEASE strip those email addresses out before doing the forward.
- Don't fall for tricks of "send this to a bunch of people and you'll receive a prize" type of emails. Trust me, you won't, although you and all your friends might receive something else (more spam!).
- Also, and least obvious, many spam messages include a way for you to opt out of future messages. Sounds good, but don't fall for it. If you reply, you've confirmed that you are a valid address for the spammer and his friends! (Sure, it SAYS you'll be removed, but don't expect it. There is an interesting flaw in the law.)



One other way you can help

In the past, we've suggested the best thing to do with spam is simply delete it and forget about it. That's still OK advice, although we're going to now request that you consider something else. In Outlook Public Folders, under:

All Public Folders \ Helpdesk

there is a folder named Spam Samples. If you'll move any spam you receive into that folder, perhaps we can find some commonalities that will help us eliminate any future spam of the same type or from the same sources.

As usual, if you have questions, please contact helpdesk.



contact us to see what we can do for your Church.
www.plumbfish.org or 770-442-1337